

KELLEY DRYE & WARREN LLP

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400

3050 K STREET, NW

WASHINGTON, D.C. 20007-5108

(202) 342-8400

FACSIMILE

(202) 342-8451

www.kelleydrye.com

NEW YORK, NY
TYSONS CORNER, VA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES
MUMBAI, INDIA

October 19, 2006

VIA ECFS

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Notice of Ex Parte Presentation, CC Docket No. 96-115, RM-11277

Dear Ms. Salas:

XO Communications ("XO"), through its attorneys, respectfully submits this notice of *ex parte* presentation. On October 18, 2006, Lisa Youngers and Tokë Vandervoort from XO Communications and the undersigned, counsel to XO, met with the following persons to discuss the Notice of Proposed Rulemaking in the above-referenced proceeding: Bill Dever, Carrie Collier-Brown, Adam Kirschenbaum, Jon Reel, Cindy Spiers, and Tim Stelzig.

During the meeting, XO distributed the attached presentation, which summarizes the scope of its presentation; the content thereof is and XO's oral remarks were consistent with the comments and replies XO submitted previously in this proceeding. In particular, XO urged the Commission not to adopt a rule that would require carriers to implement customer-set passwords. XO discussed its current security and authentication policies, and explained that customer-set passwords simply are unnecessary and might otherwise compromise effective authentication measures. In support of its position, XO explained that, to the best of its knowledge, it has not been the victim of pretexting.

XO further explained that it would be extremely costly and burdensome for carriers to implement customer-set passwords, that have not, in any event, been proven effective in preventing pretexting. XO explained that it cannot simply add a password to a field in a customer's account. Instead, XO would need to revise its current database or design a new database to house and manage the passwords. Such changes would require expensive, complex and time-consuming software and hardware augments, in addition to the resources that would be

Marlene Dortch
October 19, 2006
Page Two

needed to develop them. Moreover, XO then would need to assign full-time personnel to manage the database and to address customer inquiries regarding lost passwords (which only create new opportunities for pretexters).

XO further explained that requiring carriers to incur these substantial operational costs (which inevitably would be passed through to customers) would not result in any appreciable benefit with regard to protecting customers from pretexting. Adding costs and raising rates with no benefit is the essence of bad regulation. Indeed, the implementation of passwords, which frequently are forgotten or lost and need to be replaced, actually may result in a decreased level of security for customer information. If a carrier already maintains effective authentication standards, then substituting or augmenting with customer-set passwords does not add to the level of security provided. Instead, introduction of passwords could diminish the security of customer information, as such passwords are more likely to be defeated and create more vulnerability than the "challenge questions" included in effective authentication procedures.

This is particularly true in the case of business customers, as multiple account administrators within the company likely would have access to the password thus resulting in greater data vulnerability. Indeed, although XO does not support the requirement of mandatory passwords or the mandatory offering of optional customer-set passwords for any customer, XO emphasized that, if the Commission were to adopt a requirement that carriers make available customer-set passwords, then it must limit the requirement so that it applies only to residential customers. Passwords are particularly unworkable in the business customer context, largely because business customers are likely to have multiple authorized administrators on a single account. If XO were to assign a single password to the business customer and the customer were to lose the password or to share the password inappropriately, then XO would need to expend time and resources to reset the password for the entire company. Doing so not only would be costly and burdensome for XO, but also would interfere with the customer's legitimate requests to obtain information about its account. In short, passwords are more susceptible to being compromised in the business customer environment.

XO also explained that the publicized cases of pretexting have not involved landline business customer accounts and noted that the difficulty of tracing any call detail to particular users within an enterprise would make such information less attractive to pretexters.

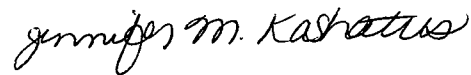
In sum, XO urged the Commission to reject each of EPIC's proposals, as all are burdensome and costly and none would be particularly effective in preventing pretexting or other already unlawful activity designed to defeat carriers' largely effective practices in protecting CPNI. Instead, the Commission should monitor the industry's efforts to arrive at industry solutions and best practices aimed at protecting the privacy of customer records.

KELLEY DRYE & WARREN LLP

Marlene Dortch
October 19, 2006
Page Three

Please contact either of us at 202-342-8400 if you have any questions regarding this filing.

Respectfully submitted,

A handwritten signature in cursive script, reading "Jennifer M. Kashatus".

John J. Heitmann
Jennifer M. Kashatus

cc: Bill Dever (via email)
Carrie Collier-Brown (via email)
Adam Kirschenbaum (via email)
Jon Reel (via email)
Cindy Spiers (via email)
Tim Stelzig (via email)

Attachment

XO Communications

Ex Parte Presentation – CC Docket No. 96-
115, RM-11277

October 18, 2006

Summary

- ❑ There is no need to modify the FCC's existing CPNI rules – the FCC's current rules are sufficient to safeguard CPNI
- ❑ The FCC should not adopt any of EPIC's proposals
- ❑ The FCC also should not modify its rules pertaining to joint venture partners and independent contractors
- ❑ XO supports the adoption of a safe harbor

There is No Need to Modify the FCC's Current CPNI Rules

- Comments in this proceeding demonstrate an overwhelming carrier commitment to consumer privacy
- Comments in this proceeding also demonstrate that the risk to customer privacy is due to pretexting or other unlawful practices

The FCC Should Not Adopt Any of EPIC's Proposals

- ❑ Adoption of EPIC's proposals would cause carriers to incur significant costs without addressing the underlying problem: pretexting
- ❑ Customer-set passwords
 - Passwords are unworkable for business customers because the implementation of customer-set passwords on accounts with multiple administrators would be extremely costly and difficult to administer
 - Consumers do not want passwords
- ❑ Audit trails
 - FCC already has rejected the use of audit trails and there is no reason to revisit that decision
 - It would be extremely costly and burdensome for carriers to change or modify their databases to be able to implement audit trails

The FCC Should Not Adopt Any of EPIC's Proposals (cont.)

- ❑ Encryption
 - Unnecessary if a carrier maintains appropriate CPNI safeguards
 - Unworkable – the carrier would need to unencrypt the data each time it needed to access the data
 - Once the carrier unencrypts the data (for example, for billing purposes), the data is now available in a written unencrypted format outside of the carrier's system, thus negating the benefits of encrypting the data
 - Prohibitively costly and nearly impossible for to implement an encryption system – would require complete replacement of carrier billing practices
- ❑ CPNI Breach Notification
 - FCC should not require carriers to notify customers each time a breach has occurred
 - Not all CPNI breaches result in the misuse of data
 - Puts an undue burden on carriers; carriers may not have knowledge that a breach has occurred
 - If a security breach has resulted in the breach of personally identifiable information (such as social security number or credit card number) and carriers have knowledge of the breach, then carriers already are required to notify consumers that a breach has occurred under various federal and state statutes
 - If the FCC implements a breach notification rule, then it must limit breach notification duties to when carriers have knowledge that the customer's own personal and credit information has been compromised; carriers should not be required to notify customers after each release of CPNI

The FCC Should Not Modify Carrier Obligations with Regard to Joint Venture Partners and Independent Contractors

- ❑ There is no evidence that fraudulent access to records is due to joint venture partners or independent contractors
- ❑ Modifying the rules pertaining to independent contractors and joint venture partners would have an adverse impact on carrier operations by shutting down independent sales channels
- ❑ Modifying the rules would violate the First Amendment of the U.S. Constitution

XO Supports Adoption of a Safe Harbor

- ☐ XO supports a safe harbor, in theory, but neither AT&T nor Verizon has fleshed out the details of its proposed safe harbor with sufficient specificity
- ☐ AT&T Safe Harbor
 - XO supports the following components of AT&T's safe harbor proposal
 - ☐ Requiring carriers to develop written procedures and to conduct training
 - ☐ Requiring carriers to develop standards for customer authentication
 - XO does not support the following components of AT&T's safe harbor proposal:
 - ☐ Optional password protection – as stated above, permitting customers to use a password would require XO to modify its databases and direct resources to administer those databases all at a significant cost to the carrier
 - ☐ Customer notification of unauthorized access/disclosure of CPNI
- ☐ Verizon Safe Harbor
 - XO supports the following components of Verizon's safe harbor proposal
 - ☐ Posting privacy practices on carrier websites
 - ☐ Filing CPNI certifications with the FCC annually
 - ☐ Developing detailed security procedures and training employees in the use of those procedures
 - ☐ Refraining from providing social security numbers and billing addresses to anyone other than the account holder
 - ☐ Verifying the identity of the account holder
 - For the reasons stated above, XO does not support Verizon's proposal to implement optional password protection for consumers – any optional password safe harbor should be limited to residential customers

Additional Considerations

- XO supports COMPTEL's request that the FCC affirmatively prohibit language in commercial agreements that would require CLECs to relinquish their control over customer CPNI
 - Contract provisions proposed in AT&T commercial agreements interfere with a CLEC's ability to protect its customer's CPNI
 - FCC should confirm that language in AT&T's (or any other commercial agreement) that hampers a carrier's ability to protect its customers' CPNI would be deemed unenforceable
- FCC should not apply CPNI rules to ISPs or information services
 - Doing so is not supported by section 222, which applies solely to information derived from "telecommunications services"
 - Applying CPNI requirements to information services is not necessary; EPIC is concerned about the release of telephone call records, and has not demonstrated any basis for applying CPNI requirements to ISPs or information services